(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 738 436**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **95 03572**

(51) Int Cl⁶ : H 04 L 9/28, G 08 C 19/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 22.03.95.

(30) **Priorité** : 06.03.95 FR 9502781.

(43) **Date de la mise à disposition du public de la demande :** 07.03.97 Bulletin 97/10.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *NOVELLA CARMELO* — FR.

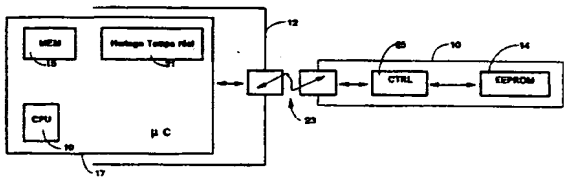
(72) **Inventeur(s) :**

(73) **Titulaire(s) :**

(74) **Mandataire :** DE BEAUMONT.

(54) SYSTEME DE CONTROLE D'ACCES PAR CLE ELECTRONIQUE PORTABLE.

(57) La présente invention concerne un système de contrôle d'accès à clé électronique (10) munie d'une mémoire (14) accessible par un appareil de contrôle d'accès (12) et stockant un code d'accès destiné à autoriser un accès auprès d'un appareil de contrôle d'accès ayant un code correspondant. La mémoire de la clé est susceptible de stocker une autorisation de modification du code de l'appareil de contrôle, la validité de cette autorisation de modification étant limitée dans le temps.



FR 2 738 436 - A1

SYSTÈME DE CONTRÔLE D'ACCÈS PAR CLÉ ÉLECTRONIQUE PORTABLE

La présente invention concerne un système de contrôle d'accès à clé électronique, dans lequel un appareil de contrôle d'accès vérifie qu'un code contenu dans une clé électronique qui lui est présentée est bien un code en vigueur dans l'appareil pour autoriser ou non un accès au porteur de la clé.

Dans un système de contrôle d'accès très répandu, les codes, de l'appareil de contrôle et de la clé, sont programmés à l'aide de micro-interrupteurs. Le code de la clé peut être transmis vers l'appareil de contrôle de diverses manières, par exemple, par contact électrique, par transmission optique, etc.

Pour préserver la sécurité du système lorsqu'une clé est perdue, le code de l'appareil de contrôle d'accès doit être modifié, et par conséquent on doit aussi modifier les codes de toutes les autres clés qui permettent l'accès auprès de cet appareil.

Dans certains cas, une même clé, ou groupe de clés, a accès auprès de plusieurs appareils de contrôle. Alors, dans le cas d'une perte de clé, le code de tous les appareils de contrôle et de toutes les clés doit être modifié. Cette opération de modification de code représente une tâche considérable si les clés et les appareils de contrôle sont nombreux.

Un objet de la présente invention est de prévoir un système de contrôle d'accès par clé électronique qui permette une modification particulièrement aisée de codes d'accès, notamment dans le cas où une ou plusieurs clés électroniques permettent l'accès auprès de plusieurs appareils de contrôle.

Pour atteindre cet objet, la présente invention prévoit une clé électronique munie d'une mémoire accessible par un appareil de contrôle d'accès et stockant un code d'accès destiné à autoriser un accès auprès d'un appareil de contrôle d'accès ayant un code correspondant. La mémoire de la clé est susceptible de stocker une autorisation de modification du code de l'appareil de contrôle, la validité de cette autorisation de modification étant limitée dans le temps.

Selon un mode de réalisation de la présente invention, la mémoire de la clé stocke un code courant correspondant au code d'un appareil de contrôle d'accès et un nouveau code avec une autorisation de modification du code courant par le nouveau code dans l'appareil de contrôle d'accès.

Selon un mode de réalisation de la présente invention, la mémoire de la clé stocke une date d'expiration de l'autorisation de modification.

Selon un mode de réalisation de la présente invention, la mémoire de la clé comprend plusieurs emplacements associés à des niveaux d'accès respectifs, un emplacement étant susceptible de stocker un code de niveau correspondant qui autorise l'accès auprès d'un appareil de contrôle d'accès ayant en vigueur le même code pour le même niveau.

La présente invention vise également un procédé d'autorisation d'accès à partir d'une clé électronique munie

d'une mémoire stockant un code. Il comprend les étapes consistant à lire dans la mémoire de la clé une autorisation de modification d'un code en vigueur et, si une telle autorisation est présente, modifier le code en vigueur à condition qu'un délai d'autorisation de modification de code ne soit pas expiré.

Selon un mode de réalisation de la présente invention, le procédé comprend l'étape consistant à lire dans la mémoire de la clé un code courant, un nouveau code, et une autorisation de modification de code de durée limitée. Si la durée de l'autorisation de modification n'a pas expiré et si le code en vigueur correspond au code courant, le code en vigueur est remplacé par le nouveau code.

Selon un mode de réalisation de la présente invention, le procédé comprend l'étape consistant à lire dans la mémoire de la clé une date d'expiration d'autorisation et à comparer cette date à une date indiquée par une horloge.

Selon un mode de réalisation de la présente invention, le procédé comprend l'étape consistant, lorsqu'une autorisation de modification est présente dans la clé, à initialiser le décomptage du délai d'expiration par un temporisateur.

Ces objets, caractéristiques et avantages ainsi que d'autres de la présente invention seront exposés en détail dans la description suivante de modes de réalisation particuliers, faite à titre non limitatif à l'aide des figures jointes parmi lesquelles :

la figure 1 représente schématiquement une clé et un appareil de contrôle d'accès selon la présente invention ;

la figure 2 représente un premier exemple d'organigramme des opérations effectuées lors d'un contrôle d'accès et d'une modification de code selon la présente invention ;

la figure 3 illustre une organisation hiérarchisée d'appareils de contrôle accessibles par des clés à différents niveaux de codes ; et

la figure 4 représente un deuxième exemple d'organigramme d'opérations effectuées lors d'un contrôle d'accès et d'une modification de code selon la présente invention.

La figure 1 représente une clé électronique 10 coopérant avec un appareil de contrôle d'accès 12. Selon l'invention, la clé 10 et l'appareil de contrôle 12 stockent un code d'accès dans une mémoire non volatile, 14 dans la clé 10 et 15 dans l'appareil de contrôle 12. La mémoire 14 est par exemple de type EEPROM et la mémoire 15 est, par exemple, celle d'un micro-contrôleur 17 alimenté en permanence. Le micro-contrôleur 17 comprend en outre une unité de traitement 19, une horloge temps réel ou temporisateur 21 et communique avec la clé 10 par une interface 23.

La clé 10 est entièrement passive, c'est-à-dire qu'elle n'échange de données entre sa mémoire 14 et l'interface 23 qu'en recevant des ordres par l'interface 23. Un circuit de commande 25 permet de traduire les ordres et d'opérer les échanges entre la mémoire 14 et l'interface 23.

L'interface 23 peut être de tout type classique. De préférence, afin qu'il ne soit pas nécessaire d'alimenter la clé 10 de manière autonome, l'interface 23 est un contact électrique qui permet d'alimenter la clé 10 à partir de l'alimentation de l'appareil de contrôle 12 en même temps que l'échange d'informations entre la mémoire 14 et le micro-contrôleur 17.

Le fonctionnement normal de ce système est, par exemple, le suivant. Le micro-contrôleur 17 émet, par l'interface 23, un ordre de lecture de la mémoire 14 d'une clé. Si la réponse n'arrive pas avant un certain délai, parce qu'une clé 10 n'est pas présente, le micro-contrôleur 17 émet un nouvel ordre de lecture, et ainsi de suite. Si une clé 10 est présente, le micro-contrôleur 17 reçoit le code stocké dans la mémoire 14 de la clé. Ce code est comparé à celui en vigueur qui est stocké dans la mémoire 15 et, si les deux codes coïncident, l'accès est autorisé.

Pour permettre une modification particulièrement aisée du code en vigueur de l'appareil de contrôle, stocké dans la mémoire 15, la présente invention prévoit de stocker dans la mémoire 14 d'une clé, sous forme d'un code spécifique, une autorisation de modification du code en vigueur dans l'appareil de contrôle 12. Le code et l'autorisation sont fournis à la clé 10, par exemple, en présentant la clé à un programmateur centralisé ayant également une interface 23 et dont l'accès est réservé à des personnes autorisées.

La figure 2 représente un organigramme d'un premier exemple d'opérations effectuées par le micro-contrôleur 17 lors d'un contrôle d'accès et d'une modification de code.

Lorsque la clé est présentée devant l'appareil de contrôle 12, le micro-contrôleur 17, en 100, lit dans la mémoire 14 de la clé le code et une éventuelle autorisation de modification.

Si le code n'est pas bon en 102, c'est-à-dire si le code de la clé ne correspond pas à celui de l'appareil de contrôle, on vérifie en 104 la présence de l'autorisation de modification et si celle-ci est valide. Pour déterminer la validité d'une autorisation de modification, cette dernière est, par exemple, écrite dans la mémoire 14 avec une date d'expiration. Cette date est alors lue par le micro-contrôleur 17 et comparée à la date indiquée par l'horloge temps réel 21. La seule présence de la date d'expiration dans la clé peut constituer l'autorisation.

En 106, si l'autorisation n'est pas valide, ou si celle-ci n'existe pas, elle est annulée et l'accès est refusé en 108.

Si l'autorisation est valide, le micro-contrôleur remplace, en 110, le code stocké dans la mémoire 15 par le code lu dans la mémoire 14 de la clé et autorise l'accès en 112.

Si le code est bon en 102, le micro-contrôleur vérifie aussi, en 114, si l'autorisation de modification est valide.

Si oui, l'accès est directement autorisé. Par contre, si l'autorisation n'est pas valide, celle-ci est annulée en 116 avant d'autoriser l'accès.

En pratique, une autorisation de modification est supposée valide tant que la date indiquée par l'horloge temps réel 21 est inférieure à la date d'expiration contenue dans la mémoire 14 de la clé. Toutefois, comme l'horloge temps réel 21 déborde périodiquement et recommence à compter à partir de 0, il est nécessaire d'assurer que les autorisations de modification soient annulées (en 106 et 116) avant que l'horloge temps réel 21 ne déborde. Sinon, une autorisation non-valide deviendrait de nouveau valide.

Avec ce fonctionnement, l'utilisation du système se résume de la manière suivante. Un utilisateur perd sa clé 10. Il se munit alors d'une clé 10 vierge et la présente au programmateur centralisé qui charge dans la mémoire 14 de cette clé un nouveau code et une autorisation de modification avec sa date d'expiration. L'utilisateur peut alors, jusqu'à la date d'expiration, reprogrammer chacun des appareils de contrôle 12 avec le nouveau code contenu dans sa clé. Passé le délai d'expiration, si la clé est présentée à un appareil de contrôle 12, celui-ci, au lieu de modifier son code en vigueur, annule dans la clé l'autorisation de modification.

Il est indispensable que l'autorisation de modification soit limitée dans le temps, car cette autorisation de modification permet en fait l'accès à n'importe quelle clé, notamment à des clés perdues illicitement utilisées.

Bien entendu, il est possible qu'un utilisateur perde sa clé tandis que celle-ci est encore autorisée à modifier les codes. Dans ce cas, l'utilisateur doit attendre l'expiration de l'autorisation de la clé perdue avant de chercher à modifier de nouveau les codes. En effet, s'il modifie les codes avant la date d'expiration de la clé perdue, cette clé perdue pourrait encore modifier les nouveaux codes par derrière. Si, toutefois,

l'utilisateur ne peut pas attendre la date d'expiration de la clé perdue, il se munit, auprès du programmateur centralisé, d'une copie de la clé perdue (avec le même code et la même date d'expiration), qu'il utilisera jusqu'à la date d'expiration avant de se munir d'une clé avec un nouveau code et une autorisation de modification.

Dans le cas où des nouveaux appareils de contrôle d'accès 12 sont installés et doivent être accessibles par les clés déjà existantes, ces nouveaux appareils de contrôle ont en vigueur un code de base que chaque clé 10 stocke également de manière permanente. Ces codes de base sont, par exemple, chargés en usine dans les appareils et les clés. Les micro-contrôleurs 17 des nouveaux appareils de contrôle liront le code de base dans une clé qui leur est présentée sans autorisation de modification, afin de permettre l'accès. Ensuite, l'utilisateur à qui sont affectés les nouveaux appareils de contrôle présentera sa clé au programmateur centralisé afin de charger dans la clé une autorisation de modification. Alors, au moment où l'utilisateur représente sa clé aux nouveaux appareils de contrôle, ceux-ci remplacent leur code de base par le code de la clé, code qui était en vigueur dans les autres appareils affectés à l'utilisateur.

Un système de contrôle d'accès selon l'invention est particulièrement avantageux lorsque les appareils de contrôle sont des serrures d'entrées d'immeubles qui doivent être accessibles aux facteurs pour déposer le courrier dans les boîtes à lettres. Alors, le programmateur centralisé se trouve à l'endroit où les facteurs récupèrent le courrier à distribuer de manière qu'ils puissent, le cas échéant, reprogrammer leur clé juste avant de faire leur tournée. L'opération la plus complexe que doit effectuer un facteur est de présenter la clé de temps en temps au programmateur centralisé. Toutes les autres opérations, notamment de modification de code, sont transparentes et rendent l'emploi du système particulièrement agréable.

Lorsqu'un grand nombre d'appareils de contrôle d'accès doit être accessible à un nombre relativement important de personnes, on souhaite, pour augmenter la sécurité, répartir les personnes par groupes qui n'ont accès qu'auprès d'un nombre limité d'appareils de contrôle. Par exemple, on affecte à un groupe de facteurs le seul secteur qu'ils couvrent lors d'une tournée.

La figure 3 représente schématiquement plusieurs de ces secteurs, chaque secteur comportant plusieurs appareils de contrôle accesibles par un code spécifique C1 de niveau 1 (C1-1, C1-2...). Plusieurs secteurs sont accessibles par un code spécifique C2 de niveau 2 (C2-1, C2-2). Plusieurs niveaux 2 sont accessibles par un code spécifique C3 de niveau 3 (C3-1), etc.

Ce sont les appareils de contrôle eux-mêmes qui établissent cette hiérarchie. Pour cela, chaque appareil de contrôle stocke les codes de niveaux successifs qui lui sont attribués. Par exemple, les appareils accessibles par le code C1-1 stockent également les codes C2-1 et C3-1.

Une clé de niveau i (i = 1, 2...), c'est-à-dire une clé permettant d'accéder à tous les appareils d'une branche hiérarchique de code Ci, stocke ce code à un emplacement réservé au niveau i. Par exemple, une clé ayant accès aux secteurs de codes C1-1 et C1-2, se trouvant dans la branche de code C2-1, stocke le code C2-1 à l'emplacement réservé au niveau 2. En fait, les clés, toutes similaires, ont un emplacement réservé à chaque niveau, et c'est seulement l'un de ces emplacements qui, en utilisation normale, est occupé par un code correspondant.

Maintenant, si une clé doit modifier un code de niveau n (n = 1, 2...), elle stocke le code de niveau n en vigueur C_{n0} ainsi que le nouveau code C_{n1}, ces deux codes étant chargés par le programmateur centralisé à l'emplacement de la clé réservé au niveau n. Bien entendu, comme dans le cas de la figure 2, la clé reçoit une autorisation de modification ayant une validité limitée dans le temps. Cette autorisation peut être contituée par la

simple présence du couple de codes Cn_0 et Cn_1. Le niveau n du code à modifier n'est pas forcément le niveau i de la clé, ce qui signifie qu'une clé de niveau quelconque peut modifier, en toute sécurité, un code de niveau quelconque de manière transparente pour l'utilisateur.

La figure 4 représente un organigramme des opérations effectuées par l'appareil de contrôle d'accès 12 pour traiter une telle clé.

En 200, le micro-contrôleur parcourt la mémoire 14 de la clé. Il y trouve le code Ci de la clé et, le cas échéant, le code courant à modifier Cn_0 (pouvant être le code Ci), le nouveau code Cn_1 et l'autorisation de modification. Le code de la clé et le code à modifier sont différenciés par le fait qu'il y a un seul code (celui de la clé) à l'emplacement de niveau i et un couple de codes à l'emplacement de niveau n. Les niveaux i de la clé et n du code à modifier sont quelconques, le traitement étant identique, quel que soit le niveau du code à modifier.

En option, on peut refuser qu'une clé utilisée auprès d'un appareil de contrôle qui ne lui est pas associé (le code Ci est mauvais) modifie le code Cn_0. Dans ce cas, si le code Ci est mauvais, l'accès est refusé en 201 sans modification du code Cn_0.

Les codes Cn_0 et Cn_1 sont comparés, en 202, au code en vigueur de niveau n stocké dans la mémoire 15 de l'appareil de contrôle.

Si aucun des codes Cn_0 et Cn_1 ne correspond au code en vigueur de niveau n, on vérifie, en 204, si le code Ci est bon. Si oui, l'accès est autorisé en 205, sinon, l'accès est refusé en 201. Selon une variante, on pourra en même temps vérifier la validité de l'autorisation de modification et annuler celle-ci si sa durée a expiré.

Si le code courant Cn_0 correspond au code de niveau n en vigueur, l'appareil de contrôle 12 est l'un de ceux dont il faut modifier le code de niveau n. Si le nouveau code Cn_1 cor-

respond au code de niveau n en vigueur dans l'appareil de contrôle, cela signifie qu'une clé a déjà reprogrammé l'appareil. Dans les deux cas, on vérifie en 206 si l'autorisation de modification est valide. Si l'autorisation de modification est valide, le code en vigueur de niveau n est remplacé par le nouveau code Cn_1 en 210, et l'accès est autorisé ou non selon la valeur du code Ci en 204. Si le code Ci de la clé est le code à modifier Cn_0, on vérifie également en 204 si le nouveau code Cn_1 est celui en vigueur, de manière à permettre l'accès à une clé qui vient de programmer l'appareil de contrôle avec le nouveau code Cn_1.

Si l'autorisation n'est pas valide, elle est annulée en 208 et on autorise ou non l'accès selon la valeur du code Ci en 204. L'autorisation est de préférence annulée en 208 si l'on utilise le système à date d'expiration décrit en relation avec la figure 2 pour déterminer la validité de l'autorisation. Si l'autorisation est constituée par la simple présence du couple de codes Cn_0 et Cn_1 dans la clé, l'annulation de l'autorisation consiste à effacer les codes Cn_0 et Cn_1. Si le code Cn_0 est le code de la clé (Cn_0=Ci), celui-ci est effacé, de manière à laisser subsister uniquement le nouveau code Cn_1 qui devient le code de la clé.

Pour vérifier la validité de l'autorisation de modification en 206, on utilise, de préférence, le système décrit en relation avec la figure 2, c'est-à-dire que l'autorisation de modification est chargée dans une clé avec une date d'expiration, cette date d'expiration étant comparée à la date indiquée par l'horloge temps réel 21 du micro-contrôleur. En effet, ce système permet au programmateur centralisé de modifier la durée de validité de l'autorisation de modification selon les besoins.

On pourrait aussi utiliser le système suivant pour vérifier la validité d'une autorisation de modification. Lorsqu'une clé avec une autorisation de modification est présentée pour la première fois à un appareil de contrôle, le micro-con-

trôleur initialise dans l'horloge 21 le décomptage d'une durée de validité prédéfinie tandis qu'il remplace le code Cn_0 en vigueur dans la mémoire 15 par le nouveau code Cn_1. Si la même clé est présentée de nouveau à l'appareil de contrôle après l'expiration de la durée de validité, le micro-contrôleur détecte, grâce à l'égalité entre le code Cn_1 maintenant en vigueur dans l'appareil et le "nouveau" code Cn_1 dans la clé, que c'est bien l'autorisation de modification de cette clé qui a expiré.

Les opérations à effectuer avec les clés en cas de perte sont les mêmes que celles décrites en relation avec la figure 2. Toutefois, le programmateur centralisé est relativement plus complexe car il stocke la hiérarchie de la figure 3 ainsi que chacun des codes en vigueur correspondants de manière à pouvoir identifier une clé par son code et lui fournir, le cas échéant, des nouveaux codes appropriés à modifier.

Si une clé de niveau n supérieur à 1 est perdue, toutes les clés de niveau inférieur ou égal à n reçoivent du programmateur centralisé le code Cn_0 de niveau n à modifier et le nouveau code Cn_1 de niveau n avec une autorisation de modification, la clé stockant toujours le code en vigueur Ci correspondant à son niveau i. Lorsque la clé est présentée devant un appareil de contrôle 12, les modifications, le cas échéant, ne s'effectuent que sur le code de niveau n selon l'organigramme de la figure 4. Indépendamment des modifications des codes, l'accès est seulement autorisé si le code Ci est bon. Ceci peut autoriser, même à des clés qui n'ont pas l'autorisation d'accès, de modifier des codes de niveaux différents en toute sécurité, ce qui permettra une modification plus rapide des codes par des personnes qui, involontairement ou intentionnellement, utilisent une mauvaise clé.

REVENDICATIONS

1. Clé électronique (10) munie d'une mémoire (14) accessible par un appareil de contrôle d'accès (12) et stockant un code d'accès destiné à autoriser un accès auprès d'un appareil de contrôle d'accès ayant un code correspondant, caractérisée en ce que sa mémoire est susceptible de stocker une autorisation de modification du code de l'appareil de contrôle, la validité de cette autorisation de modification étant limitée dans le temps.

2. Clé électronique selon la revendication 1, caractérisée en ce qu'elle stocke un code courant (Cn_0) correspondant au code d'un appareil de contrôle d'accès et un nouveau code (Cn_1) avec une autorisation de modification du code courant par le nouveau code dans l'appareil de contrôle d'accès.

3. Clé électronique selon la revendication 1, caractérisée en ce que sa mémoire stocke une date d'expiration de l'autorisation de modification.

4. Clé selon la revendication 2, caractérisée en ce que sa mémoire comprend plusieurs emplacements associés à des niveaux d'accès respectifs, un emplacement étant susceptible de stocker un code (Ci) de niveau correspondant qui autorise l'accès auprès d'un appareil de contrôle d'accès ayant en vigueur le même code pour le même niveau.

5. Procédé d'autorisation d'accès à partir d'une clé électronique (10) munie d'une mémoire (14) stockant un code, caractérisé en ce qu'il comprend les étapes consistant à lire dans la mémoire de la clé une autorisation de modification d'un code en vigueur et, si une telle autorisation est présente, modifier le code en vigueur à condition qu'un délai d'autorisation de modification de code ne soit pas expiré.

6. Procédé selon la revendication 5, caractérisé en ce qu'il comprend les étapes suivantes :

- lire dans la mémoire de la clé un code courant (Cn_0), un nouveau code (Cn_1), et une autorisation de modification de code de durée limitée ; et

- si la durée de l'autorisation de modification n'a pas expiré et si le code en vigueur correspond au code courant, remplacer le code en vigueur par le nouveau code.

7. Procédé selon la revendication 5, caractérisé en ce qu'il comprend l'étape consistant à lire dans la mémoire de la clé une date d'expiration d'autorisation de modification et comparer cette date à une date indiquée par une horloge (21).

8. Procédé selon la revendication 6, caractérisé en ce qu'il comprend l'étape consistant, lorsqu'une autorisation est présente dans la clé, à initialiser le décomptage du délai d'expiration par un temporisateur (21).

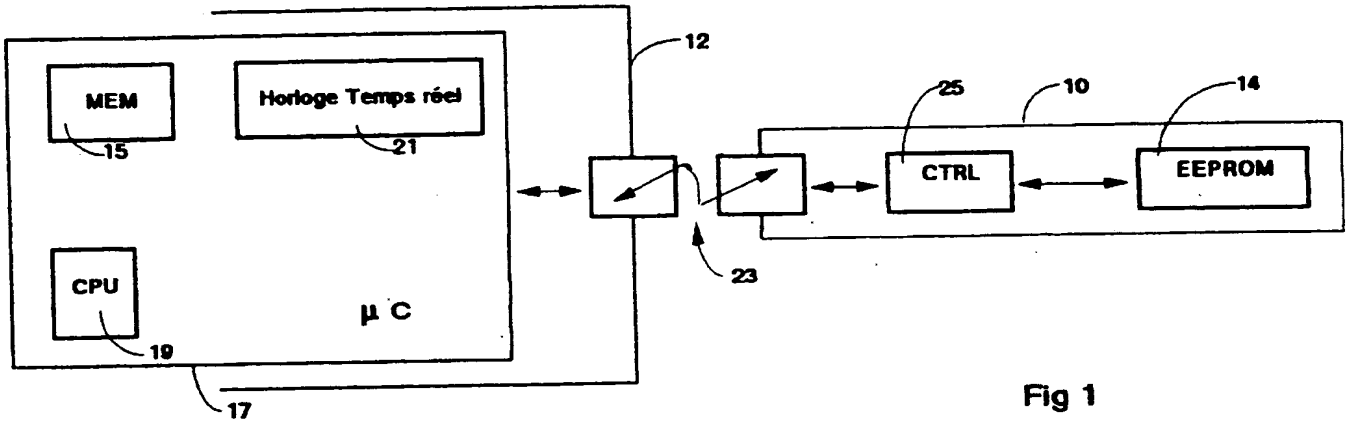

MEM
15
Horloge Temps réel
21
12
25
10
14
CTRL
EEPROM
23
CPU
19
µ C
17

Fig 1

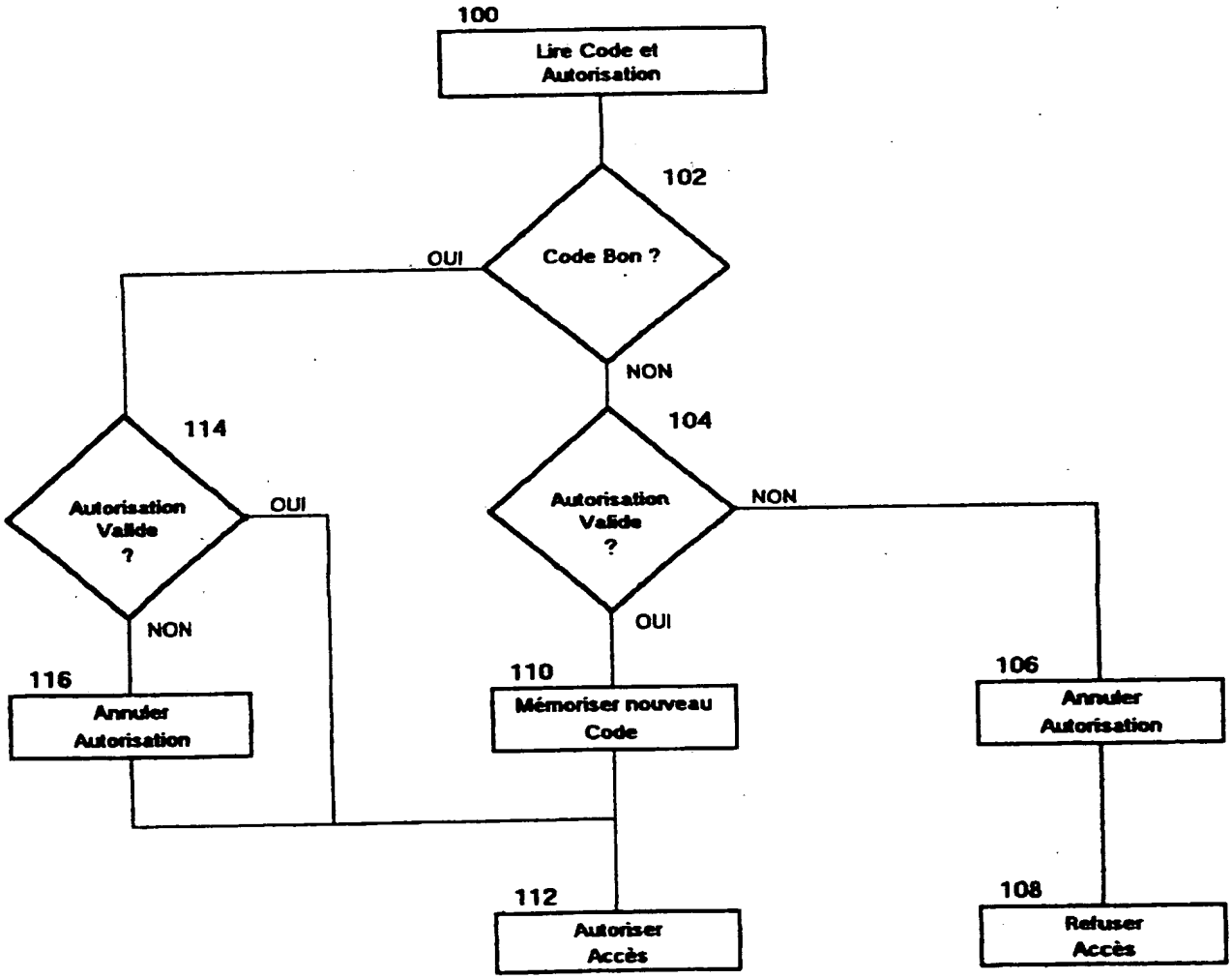

100
Lire Code et Autorisation
102
Code Bon ?
OUI
NON
114
Autorisation Valide ?
OUI
NON
104
Autorisation Valide ?
NON
OUI
116
Annuler Autorisation
110
Mémoriser nouveau Code
106
Annuler Autorisation
112
Autoriser Accès
108
Refuser Accès

Fig 2

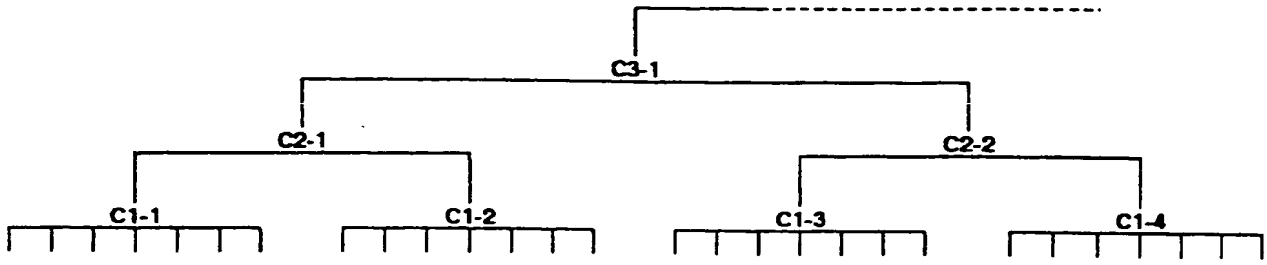


Fig 3

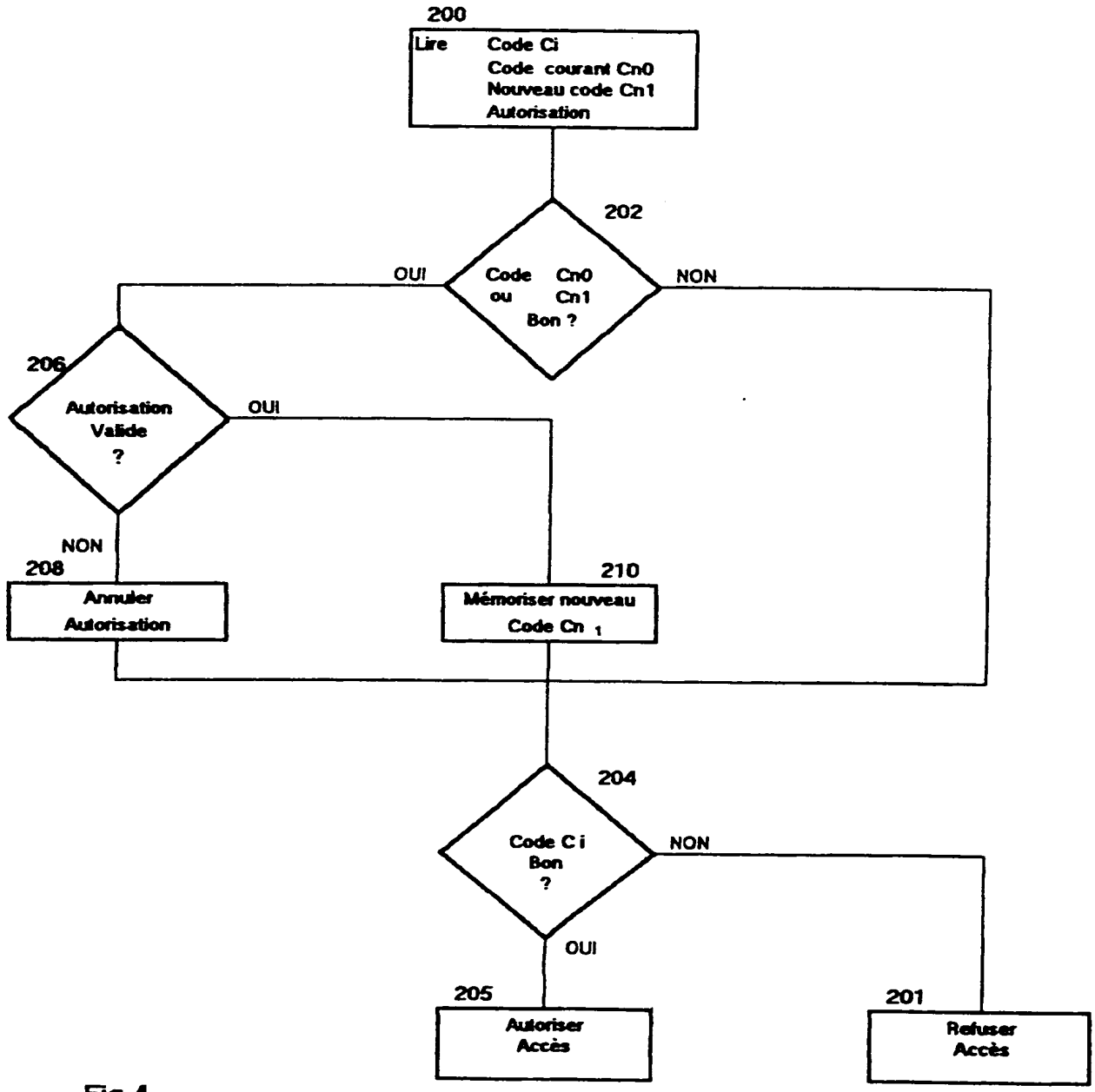


Fig 4

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2738436
N° d'enregistrement national

FA 518033
FR 9503572

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	WO-A-94 15048 (TREHARNE,MOORE) * page 2, ligne 19 - page 4, ligne 28; figures 1-3 *	1,2,5,8
A	EP-A-0 122 244 (WSO CPU-SYSTEM AB) * page 7, ligne 33 - page 10, ligne 6; figures 1,2 *	1,3,5,7
A	GB-A-2 251 266 (TRIOVING) * page 2, ligne 25 - page 13, ligne 25; figures 1-7 *	1,3-7

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

E05B
G07C

Date d'achèvement de la recherche: 5 Février 1996

Examinateur: Herbelet, J.C.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

1